# The Future of Digital Evidence - Proceedings of a Strategic Conversation

Nic Daeid, Niamh; Marra, Michael

*DOI:*
10.20933/100001125

*Publication date:*
2019

Leverhulme Research Centre
for Forensic Science
University of Dundee

LEVERHULME
TRUST

# THE FUTURE OF DIGITAL EVIDENCE – PROCEEDINGS OF A STRATEGIC CONVERSATION.

MAY 2019

Professor Niamh Nic Daeid
Mr Michael Marra

## Executive Summary

The ubiquitous nature of personal electronic devices and the essential part that digital data and information, both public and private plays in the lives of almost everyone means that all aspects of society, including maters of civil and criminal dispute, now have a digital element. This is set to dramatically increase in the coming years with 50 billion devices predicted to be connected through the Internet of Things by 2020. Digital data, information, transactions, functionality and access have little in common with the physical world and when it comes to securing, protecting and analysing digital evidence the application of conventional policing and investigative strategies are severely hampered if not simply not fit for purpose. This poses significant concerns to undertaking criminal investigations in an increasingly digital world.

In May of 2018, the Leverhulme Research Centre for Forensic Science (LRCFS) at the University of Dundee ran a two-day residential strategic conversation which brought together experts from Policing, the Judiciary, Industry and academia into a proactive and immersive discussion and workshop. The participants explored together the challenges that the digital nature of society presents to the collection, protection and analysis of digital evidence within the context of the justice space. Participants developed a shared perspective and co-developed three themes to progress, incorporating six initial challenges:

| | |
|---|---|
| 1. Awareness theme: | Challenge 1 - evaluating and identifying needs;<br>Challenge 2 - raising awareness for business and the public |
| 2. Pace of change theme: | Challenge 3 - triage<br>Challenge 4 - dealing with seized devices |
| 3. Operational readiness theme: | Challenge 5 - accreditation<br>Challenge 6 - training |

### Possible next steps:

1. LRCFS recommends the creation of a project team incorporating representatives from across the justice ecosystem to include the Judiciary and Legal Profession, Government, Industry, law enforcement, the third sector and academic representatives.

2. The project team should develop a strategic framework to address the identified themes and challenges organised across the three project work flows in order to improve the processes, management, governance and quality of digital data and information gathering and their transformation into, and use as, evidence within the justice process.

## Digital evidence: A strategic ecosystem

**Introduction and Background:** In May 2018 the Leverhulme Research Centre for Forensic Science convened a two-day residential 'Strategic Conversation' on Digital Evidence in partnership with colleagues from across the justice ecosystem. The scale of the transformation required for a comprehensive digital strategy for Scotland is as much one of culture as it is of capability and resource and all of these areas were explored during the strategic conversation.

The impact of technology on public protection, crime and justice is profound and accelerating. The digital nature of how crimes are committed, detected and prosecuted is a fundamental challenge to how we seek to ensure the safety and order of our society. The development of technology is creating new cultures and behaviours which the legal and enforcement systems must understand and engage with effectively. Jurisdictional boundaries are being challenged by remote perpetrators and remote victims. Data has been globalised and is 'located' everywhere through distributed systems. Ownership of data can be unclear and conceptually fraught across public and private realms.

The character, behaviour and identity of individuals online may be radically different but no less valid than their physical counterparts. The concept of personal responsibility is morphed by screens and avatars. Ideologies spread and inform each other organically and at rapid pace. Behaviours may be exhibited online through virtual reality with pertinent risks and in some cases our very conceptual grasp of criminology is being challenged.

The operational challenges for law enforcement of this trend is all encompassing and begins with how we understand what and where crime is being committed. Threat Assessments produced for the Police identify the ongoing increase in cyber enabled and cyber dependent crime globally, nationally and locally. Yet basic problems and challenges in the labelling of crime in intelligence logs indicates a nomenclature that is not fit for purpose. Statistics that inform resource allocation are skewed by the problematic proliferation of the terms: 'digital crime', 'digital evidence', 'cybercrime', 'cyber enabled', 'internet crime' and more. The reality is that the challenge is ubiquitous and that the basic link is that crimes now have a significant digital component in how they are committed, detected or prosecuted.

**Aims:**

1. To engage the full criminal justice ecosystem in a proactive workshop relating to the future of digital evidence in Scotland.

**Objectives:**

1. To develop a themed challenge list of realistic, achievable and implementable projects.
2. To create outline research and developmental pathways for each challenge identified.

**Expectation:**

1. To gain an insight into the confidence in achievability of the agreed challenges across the stakeholder community.

## Structure, Content and Attendance:

Strategic conversations are design led challenges undertaken by an invited stakeholder community. The participants also involve those with relevant expertise from outside of the stakeholder group who can bring a different and disruptive mindset to the challenges.

Strategic conversations are structured to facilitate free flowing conversations where different directions and thoughts can be unveiled and explored in a safe and participatory space. Representatives of the following organisations attended the Future of Digital Evidence Conversation held at LRCFS in the University of Dundee.

Senior Judiciary from Scotland
Senior Judiciary from Northern Ireland
Senior Judiciary from England and Wales
Crown Office Procurator Fiscal Service
Scottish Government
Scottish Enterprise
Scottish Business Resilience Centre
Australian Federal Police
National Institute for Standards and Testing, USA
Dept of forensic sciences, Washington DC. USA
Deloitte LLP
Price Waterhouse Cooper
Ernst & Young LLP
Cyan Forensics
Torchlight Ltd
Leonardo Ltd
Oil and Gas innovation Centre
Scottish Police Authority Forensic Services
Scottish Police Authority
Police Scotland
University of Edinburgh
University of Abertay
University of St Andrews
University College London
University of Dundee

**Specific identified challenges for the criminal Justice ecosystem:**

***1. The awareness challenge:*** Both the public and businesses are experiencing the changing nature of crime in real time. Cyber crime is not a future problem requiring strategic planning and preparation, it is a clear and present threat and already permeates many aspects of crime and maintaining public order. Although the underlying nature of crime and disorder; acts against the person, theft, fraud etc. etc. remains the same, digital technology is providing many new ways, tools and techniques through which crimes can be committed. Additionally, the continued rapid development of digital technology means that these new mechanisms and the threats they pose continue to adapt and evolve rapidly.

These factors have led to a profound transformation in both the nature and the mechanisms of offences being committed but also the perception of individuals and society about the scope, nature, relative threat and means of protection against this evolving nature of crime and disorder. It is clear that as a society we do not understand the true scope in types and incidence or indeed what threats they actually pose to us as individuals or organisations and most importantly how to protect ourselves against them.

The organising purpose of our laws and their enforcement is public safety. How we ensue that safety in this new age is an open question. The public visibility of some crime has diminished largely due to a migration from physical mechanisms to digital ones. However, in moving from the physical to the digital, crimes may have far less public profile but are no less damaging. The safety and stability of our communities are based on behavioural norms that do not apply in the same way online as they do in the physical world.

What should the public expect of their laws and their police force in this new digital reality? Informing those public expectations will be critical to defining what a successful strategy is. A conversation with the public must be based on a sound understanding of the technology and the challenges we collectively face. The ability to communicate these issues is undermined by an uncertain lexicon. Terms such as ‘cyber’ and ‘digital‘ are so ubiquitous as to be meaningless. While that is a recognition in itself of the pervasive nature of a ‘digital’ world it does not lessen the challenge of inexact terminology leading to an opaque discussion.

Whilst there are already many initiatives underway to highlight the threat posed by digital devices, apps and the internet, there has been less emphasis on educating both the public and industry on what to do in the event of such digitally enabled criminal activity. The strategic conversation highlighted the need to develop beyond the current level of discussion and debate which is focussed around cyber security to provide a broader societal understanding of the potential impact of digitally enable crimes and ways in which policing can be enhanced to bring offenders to justice.

***The recommendation:*** The development of an engagement strategy with both business and the public is proposed. In order to do that, an initial clear vision must be stated with a very clear definition of what is meant by the terminology used so that the emphasis is on both protection against crime and prosecution of crime in the digital world. A series of specific tasks were identified:

- Development of a clear vision of combatting crime in the digital world
- Working with partners to understand the nature of crimes where digital evidence is pertinent.
- Development of methods of intelligence gathering working in partnership with communities and the public.
- Creation of a severity scale for crime involving digital evidence.
- Development of educational tools to improve public awareness.
- Training for communities and the public to protect against vulnerability.

***2. The pace of change challenge:***

The process of change within the criminal justice system is always slow and compared to the overwhelming pace of technological change legal change may seem rigid and unagile. Criminals are not bound by legal restrictions or behavioural norms and keeping up with technologically enabled offences is ever more difficult and challenging.

Technical challenges must also be met. Crimes committed and detected are now likely to have large volumes of digital data associated with them. These may be traditional evidence types now stored in digitised form but there are also entire new categories of evidence obtainable from devices and the internet that can help to build a picture of past and ongoing events.

The sheer scale of this data requires ever growing capacity for secure storage, transfer and, critically, analysis. The use of triaging mechanisms will become increasingly important as more and more criminal events involved digital devices or when such devices are used to record crimes. Sophisticated encryption also presents technical barriers to effective modern day policing.

Artificial intelligence may yet be a critical tool in coping with the massive data challenges presented by digital evidence but it's use is also not without its own challenges in particular with regards to biases that may be built into codes used as well as ethical considerations to the application of AI to digital information.

***The recommendation:*** The development of a coherent and joined up vision across the Scottish criminal justice ecosystem is paramount where the law makers, law enforcers, legal adjudicators and the public have both a common understanding and a common agreement on how we go forward to deal with the challenges while protecting the rights of the individual. A series of specific tasks were identified:

- Discussing and agreeing across the ecosystem and public, the legal adjustments necessary to facilitate the recovery of digital devices in criminal investigations while protecting ethical and human rights.

- Development of a triage strategy for digital devices working in partnership with public and private sector.

- Working in partnership to develop specific fit for purpose tools for extraction of case relevant information.

***3. The operational readiness challenge:*** Adapting to the new digital reality presents a plethora of operational challenges. The most immediate practical challenge relates to the skills shortage within the existing police force and the common challenge of competing in a small talent pool with high paying tech firms. The development of a current conceptual framework of operation is a critical step: how do we maintain the integrity of the judicial process? What does best evidence look like for digital materials? These will inform and be informed by the direct deployment challenges of how to police online. Defining the role of the police in this domain will require a focus on the crime itself rather than the technology.

***The recommendation:*** The delivery of operational readiness for the court system is paramount and a movement to the creation of a workflow for crime investigation involving digital evidence accredited to International standards (in particular ISO 17020/17025) is highly desirable. Similarly, both the development of new training as well as the utilisation of the existing skills base within Scotland is highly desirable once the specific skills need for existing deployed staff (police officers, blue light responders, crime scene investigators, Procurators fiscal) as well as specialists in digital evidence triage and retrieval has been identified. Key tasks include;

- Working with partners to create training course material and delivery for first responders and others.

- Discussing and agreeing the required standards for admissibility of digital evidence within the courts.

- Develop the work flows for digital evidence and the necessary standard operating procedures.

- Creating the infrastructure and documentation for accreditation.

A draft of this document was shared with a number of the participants of the strategic conversation.